



**State of Alaska Cyber Security &  
Critical Infrastructure  
Cyber Advisory**

**July 6, 2009**

*The following cyber advisory was issued by the State of Alaska and was intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.*

**ADVISORY NUMBER:**

SA2009-031

**DATE(S) ISSUED:**

7/6/2009

7/14/2009 - **UPDATED**

**SUBJECT:**

Vulnerability in Microsoft Video ActiveX Could Allow Remote Code Execution

**ORIGINAL OVERVIEW:**

A vulnerability has been discovered in Microsoft Video ActiveX control that could allow a remote attacker to take complete control of a vulnerable system. ActiveX controls are small programs or animations that are downloaded or embedded in Web pages which will typically enhance functionality and user experience. Many web design and development tools have built ActiveX support into their products, allowing developers to both create and make use of ActiveX controls in their programs.

When vulnerabilities are discovered in ActiveX controls, attackers may use specially crafted web pages to exploit these vulnerabilities. Successful exploitation may result in an attacker gaining the same user privileges as the logged on user. Depending on the privileges associated with this user account, an attacker could then install programs; view, change, or delete data; or create new accounts.

Currently, there are no patches available for this vulnerability and there are reports of targeted attacks exploiting this issue on the Internet.

**JULY 14 UPDATED OVERVIEW:**

**Microsoft has released a patch for this vulnerability.**

**SYSTEMS AFFECTED:**

- Windows XP Service Pack 2
- Windows XP Service Pack 3
- Windows Server 2003 Service Pack 2

**RISK:**

**Government:**

- Large and medium government entities: **High**
- Small government entities: **High**

**Businesses:**

- Large and medium business entities: **High**
- Small business entities: **High**

**Home users: High****ORIGINAL DESCRIPTION:**

A vulnerability has been discovered in the Microsoft Video ActiveX control which is associated with the Microsoft TV technologies. This component provides support for digital TV applications and is installed on all versions of Windows XP by default. The vulnerability occurs within the 'MPEG2TuneRequest' object of ActiveX and is triggered when the object is instantiated with malformed input through the 'data' parameter. This vulnerability may be exploited if a user visits a maliciously crafted web page. Successful exploitation may result in an attacker gaining user level privileges. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Microsoft has recommended two workarounds, each of which has a different level of impact. The first recommendation is to disable DirectX Scripting in Internet Explorer. The second recommendation is to set the kill bit for the ActiveX control identified by the following class identifier:

CLSID: 0955AC62-BF2E-4CBA-A2B9-A63F772D46CF

There are confirmed reports that this vulnerability is being used for specific targeted attacks. More widespread exploitation may occur when additional details regarding this vulnerability become available.

There is no patch available at this time.

**JULY 14 UPDATED DESCRIPTION:**

**Microsoft has released a patch for this vulnerability.**

**RECOMMENDATIONS:**

We recommend the following actions be taken:

- Set the kill bit on the Class Identifier (CLSID) {CLID - 0955AC62-BF2E-4CBA-A2B9-A63F772D46CF.}; further instructions on how to set the kill bit can be found at the following location ( <http://support.microsoft.com/kb/240797> ).
- Do not visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Ensure that all anti-virus software is up to date with the latest signatures.

- Inform and educate users regarding the threats posed by attachments and hypertext links contained in emails especially from un-trusted sources.

#### **JULY 14 UPDATED RECOMMENDATIONS:**

- **Apply the patch provided by Microsoft to vulnerable systems immediately after appropriate testing.**

#### **REFERENCES:**

##### **Microsoft:**

<http://www.microsoft.com/technet/security/advisory/972890.mspx>

<http://support.microsoft.com/kb/240797>

##### **Secunia:**

<http://secunia.com/advisories/35683/>

#### **JULY 14 UPDATED REFERENCES:**

##### **Microsoft:**

<http://www.microsoft.com/technet/security/bulletin/MS09-032.mspx>

##### **CVE:**

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=2008-0015>